S
353.54
L72TRSC
1998

Legislative Audit Division

State of Montana

Report to the Legislature

March 1998

EDP Audit

STATE DOCUMENTS COLLECTION

MONTANA STATE LIBRARY
1515 E. 6th AVE.
HELENA, MONTANA 59620

Teachers' Retirement System Computer-Based Application

Teachers' Retirement Division

This report provides information regarding the Teachers' Retirement System (TRS) computer-based application. It contains five recommendations for improving controls over TRS' electronic data processing environment. These recommendations include:

- Restricting electronic access to critical files and programs.
- Documenting and testing a disaster recovery plan.
- Documenting critical application processes.

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

98DP-03

MONTANA STATE LIBRARY
3 0864 0010 3956 2

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Linda Nelson, Chair	Representative Bruce Simon, Vice Chair
Senator Sue Bartlett	Representative Beverly Barnhart
Senator Reiny Jabs	Representative Ernest Bergsagel
Senator Tom Keating	Representative A. R. "Toni" Hagener
Senator Ken Miller	Representative Bob Keenan
Senator (Vacant)	Representative Robert Pavlovich

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel
Tori Hunthausen, IT & Operations Manager

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
James Gillett, Financial-Compliance Audit

March 1998

The Legislative Audit Committee
of the Montana State Legislature:

This is our EDP audit report of the Teachers' Retirement Division's internal controls relating to its computer-based Teachers' Retirement System (TRS) application. We reviewed the division's general controls as they relate to the data processed on their minicomputer. In addition, we reviewed application controls over the TRS application. This report contains recommendations for improving EDP controls at the division. Our recommendations include improving electronic access security, documenting and testing a disaster recovery plan, and documenting critical application programs. Written responses to our audit recommendations are included in the back of the audit report.

We thank the division personnel for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Room 135, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@mt.gov

Digitized by the Internet Archive
in 2010 with funding from
Montana State Library

http://www.archive.org/details/teachersretirement1998mont

Legislative Audit Division

EDP Audit

Teachers' Retirement System Computer-Based Application

Teachers' Retirement Division

The member of the audit staff involved in this audit was Ken Erdahl.

Table of Contents

	Appointed and Administrative Officials	ii
	Report Summary	S-1
Chapter I Introduction and Background	Introduction	1
	EDP Audit General and Application Controls	1
	Audit Conclusions	1
	Audit Objectives	2
	Audit Scope and Methodology	2
	Compliance	3
	Background	3
Chapter II - General Controls	Introduction	5
	Electronic Access Controls	6
	Programmer Access to Production Programs Should be Restricted	6
	Access to Critical System Files and Programs Should be Controlled	7
	Disaster Recovery Plan Should be Documented	8
	Documentation	9
Chapter III - Application Controls	Introduction	11
	Access Controls Over Application Functions	11
Agency Response	Teachers' Retirement Division	14

Appointed and Administrative Officials

The Teachers' Retirement Division Board of Directors and Administrative Officials		Term Expires July 1
Board of Directors	James E. Cowan, Chairman	2000
	Dr. Rick Stuber	1998
	E. Joseph Cross	1999
	Virginia Egli	2001
	James Turcotte	2001
	Jima Severson	2001

Administrative Officials	David L. Senn	Executive Director
	Gary Warren	Assistant Executive Director
	Rod Sheppard	Information Systems Specialist

Introduction

This is an electronic data processing audit of controls relating to the computer-based application which processes and stores Teachers' Retirement System (TRS) information on member contributions and disbursements. We reviewed general controls over the division's minicomputer as it relates to TRS. We also evaluated application controls over TRS, and performed a review of the application documentation.

EDP Audit General and Application Controls

EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed.

We found some areas where input and output controls over the application could be improved. *Except for the identified risks, as noted in the report, we conclude general and application controls provide for controlled application processing.*

Background

The Montana Teachers' Retirement System, established by state law in 1937, currently has more than 18,200 active members and 1173 vested inactive members. Approximately 7,900 retirees or their beneficiaries were receiving retirement, disability, or survivor benefits as of July 1997. These member contributions and disbursements are maintained and processed by the TRS application, which is a commercially developed, on-line/real time application, implemented over a six-month period beginning in September 1993, and brought fully into production in February 1994.

General Controls

General controls consist of the organization's data processing structure and control, physical security, operations, system documentation, environmental controls, access controls and change controls. Access controls ensure access to system data files and programs is limited to users authorized to process or maintain the system. Access controls ensure data has been provided on a need-to-know basis and user attributes and/or privileges have been assigned only to personnel who have a legitimate need for them.

In our review of TRD's minicomputer environment, we determined general controls provide for controlled application processing.

However, we found areas where electronic access controls, hardware and system software controls, and overall documentation could be improved.

Electronic Access Controls

Access controls prevent and/or detect deliberate or accidental changes caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. The division's security officer is responsible for insuring all production files are protected, access authorizations are properly documented, and user access is limited to specific application areas where appropriate. Assigning limited access based on job duties prevents users from inadvertently or willfully executing programs, and/or changing data unrelated to their job.

Programmer Access to Production Programs Should be Restricted

TRD's system administrator is responsible for administering and managing the computer-based application. The administrator is responsible for overall application security, data integrity, and enhancements. To help facilitate system support duties, TRD has contracted the services of an outside vendor for programming and system administration support. During our review, we found that the contracted programmer has unrestricted access to the mini-computer operating system and to application production programs and data.

Because of their high degree of technical knowledge, programmers should not have access to production programs or files. Their programming activities should be restricted to test programs and files. The system administrator, not the programmer, should be responsible for transferring the tested and approved changes into production.

Division personnel stated that because of the small size of the organization, the contract programmer needs complete, unrestricted access in order to provide computer support when the system administrator is absent. At a minimum, all system or application changes made by the programmer should be logged and reviewed.

Access to Critical System Files and Programs Should be Controlled

For individual files and programs, different levels of access (read, write, execute, and delete) may be allowed within four different categories (system, owner, group, or world). The "system" category allows access through highly-privileged system accounts, usually available to the system administrator and security officer. "Owner" allows access to the user that originated the file. "Group" allows access by anyone associated with the specified group, and "world" refers to all users with access to the system.

During our review, we found read, write, execute and delete access is granted to system users through "Group" and "World" accounts, which in effect, gives all users unlimited access to these files. The files include production data files, batch execution files, and programming source code. Improper changes or deletion of these files could cause major disruptions to the daily operations of TRD. We recommend the division restrict write and delete level access to critical program files.

Disaster Recovery Plan Should be Documented

The division has not completed a formal disaster recovery plan to return the application to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a timely manner, and minimize losses due to computer down-time.

The Montana Operations Manual (MOM) section 1-0240.00, outlines agency responsibilities regarding disaster recovery. These responsibilities include assigning recovery team member responsibilities, assessing information and resource requirements necessary to maintain applications, and determining alternate procedures which may be necessary if recovery is not timely.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a complete disaster recovery plan which defines division responsibilities and requirements, the division may be unable to recover its applications in a timely manner. We recommend the division document and test formal disaster recovery procedures.

Documentation

Documentation provides a means for ensuring continuity of operations, and facilitates staff training. All parts of the system should be documented, from the system design and implementation, to the daily tasks performed by division staff. Documentation provides a level of support and reference to existing staff, and a starting point for training new or replacement staff in the event of employee turnover.

We found areas in the TRS operations where documentation could be improved. Things such as disaster recovery, systems enhancements and application changes, detailed system security guidelines, and individual employee workflow were not completely and clearly documented.

We recommend TRD review present policies and procedures, and ensure critical processes are thoroughly documented.

Application Controls

Application controls are related to the specific tasks performed by TRS's computer-based system. Application controls consist of a combination of manual and automated procedures. Input controls ensure data input is authorized, all authorized data is input, and all data input is included in processing. These procedures, along with proper assignment and control of access privileges to the system, help ensure the overall integrity of data input, processed, and maintained on the system.

We determined that application controls generally provide for controlled processing of TRD's computerized application. However, we found one area relating to access where controls could be improved.

Access Controls Over Application Functions

As part of internal controls over the various functions in TRD, the division has segregated certain tasks so that critical input and processing functions require the review and input of more than one person. Although the functions are segregated organizationally, the division has not implemented controls to ensure these conflicting duties are electronically segregated. The computer-based application gives the division the ability to separate those functions electronically, so each individual has access to perform only one of

the two tasks, and is locked out of the other. Division personnel indicated they did not feel electronic restrictions are necessary, because the individuals doing those jobs are aware of which tasks they are and are not authorized to perform. The division should implement the available electronic controls in coordination with their established organizational controls.

Chapter I - Introduction and Background

Introduction

This is an electronic data processing audit of controls relating to the computer-based application which processes and stores Teachers' Retirement System (TRS) information on member contributions and disbursements. We reviewed general controls over the division's minicomputer as it relates to TRS. We also evaluated application controls over TRS, and performed a review of the application documentation.

As of July 1997, the division had more than 18,200 active members, and assets in excess of $1.9 billion. A total of 7,901 members and beneficiaries receive retirement, disability, or survivor benefits totaling over $88 million each year.

EDP Audit General and Application Controls

EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed.

A general control review provides information about the environment in which the computer systems operate and includes an examination of controls in place over the computer applications. Applications must operate within the general control environment in order for any reliance to be placed on them.

Application controls are specific to a given computer application (a set of programs that accomplish a specific function). The review includes an examination of controls over input, processing and output.

Audit Conclusions

As discussed in Chapter II of this report, we found some areas where general controls could be improved. Application controls are discussed in Chapter III. We found some areas where input and output controls over the application could be improved. ***Except for the identified risks, as noted in the report, we conclude general and application controls provide for controlled application processing.***

Audit Objectives

The objectives of this audit were to evaluate:

1. General controls specific to the division's data processing center which processes TRS application data.

2. The effectiveness of application controls over data stored on the system and distributed through TRS.

Audit Scope and Methodology

The audit was conducted in accordance with generally accepted government auditing standards. We compared the division's general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), United States General Accounting Office (GAO), and the information technology industry.

We reviewed the division's general controls related to the computer environment. We interviewed division personnel to gain an understanding of the hardware and software environment, and examined documentation to supplement and confirm information obtained through interviews.

We also reviewed the division's application controls in relation to TRS. We reviewed input controls such as input authorization, edits, access controls, and error correction procedures. We also reviewed output controls by evaluating the accuracy and validity of data on system generated reports.

In addition, we determined if supporting documentation existed in regard to the application, outlining such things as problem definitions, systems, programs, operations, and user involvement. We reviewed the division's processes and procedures for use of the application in collecting contributions and paying benefits for all active and retired Montana teachers.

Compliance

We determined the division to be in compliance with laws applicable to collection of contributions and disbursement of benefits as tested.

Background

The Montana Teachers' Retirement System, established by state law in 1937, currently has more than 18,200 active members and 1173 vested inactive members. Approximately 7,900 retirees or their beneficiaries were receiving retirement, disability, or survivor benefits as of July 1997. These member contributions and disbursements are maintained and processed by the TRS application, which is a commercially developed, on-line/real time application, implemented over a six-month period beginning in September 1993, and brought fully into production in February 1994. There have been no prior electronic data processing audits of TRS.

A six-member retirement board governs the retirement system. The board's responsibilities include:

1. Establishing rules and regulations necessary for the proper administration and operation of the retirement system.

2. Determining the eligibility of a person who is applying for membership in the system.

3. Granting retirement, disability, and other benefits under the provisions of Title 19, chapter 20, MCA.

4. Designating an actuary to provide consultation on the technical actuarial aspects of the retirement system.

Except as noted below, all full-time members of the teaching profession are required by law to be members in the Teachers' Retirement System. An eligible employee of the university system, hired after July 1, 1993, must become a member in the Teachers' Insurance and Annuity Association - College Retirement Equities Fund (TIAA-CREF), unless the employee is already a member of the Teachers' Retirement System or the Public Employees' Retirement System.

Chapter II - General Controls

Introduction

The TRS application operates on a minicomputer. Helena TRS employees access the system via their local area network. Support responsibility for the system is under contract with an outside vendor located in California. Under this arrangement, the vendor is responsible for application and software development, maintenance, testing and integration.

Facilities management is handled in-house, and includes:

- Batch processing functions.
- User training and help desk services.
- Ad hoc inquiries; reports and extracts.
- Database file and library maintenance.
- Data backup/restoration.
- Business continuity.
- Software and hardware security administration.

General controls consist of the organization's data processing structure and control, physical security, operations, system documentation, environmental controls, access controls and change controls. Access controls ensure access to system data files and programs is limited to users authorized to process or maintain the system. Access controls ensure data has been provided on a need-to-know basis and user attributes and/or privileges have been assigned only to personnel who have a legitimate need for them.

In our review of TRD's minicomputer environment, we determined general controls provide for controlled application processing. However, we found areas where electronic access controls, hardware and system software controls, and overall documentation could be improved.

Electronic Access Controls

Access controls prevent and/or detect deliberate or accidental changes caused by improper use or unauthorized manipulation of data, programs, and/or computer resources. The division's security officer is responsible for insuring all production files are protected, access authorizations are properly documented, and user access is limited to specific application areas where appropriate. Assigning limited access based on job duties prevents users from inadvertently or willfully executing programs, and/or changing data unrelated to their job.

Access security on the system is controlled using three layers: Operating system security - used to control access to the operating system; network access security - used to control access to the network; and application security - used by the application to control specific access and user privileges to the application itself. We found several concerns relating to electronic access at the various levels of security.

Programmer Access to Production Programs Should be Restricted

TRD's system administrator is responsible for administering and managing the computer-based application. The administrator is responsible for overall application security, data integrity, and enhancements. To help facilitate system support duties, TRD has contracted the services of an outside vendor for programming and system administration support. During our review, we found that the contracted programmer has unrestricted access to the mini-computer operating system and to application production programs and data.

Industry standards suggest management prohibit programmer access to production programs and data. In addition, industry standards state that no one person should have incompatible duties that would permit the perpetration and concealment of material errors or irregularities. The present access allows the programmer the ability to change any information on the system, such as member contributions, retiree status, addresses, etc., without authorization.

Because of their high degree of technical knowledge, programmers should not have access to production programs or files. Their programming activities should be restricted to test programs and

files. The system administrator, not the programmer, should be responsible for transferring the tested and approved changes into production.

Division personnel stated that because of the small size of the organization, the contract programmer needs complete, unrestricted access in order to provide computer support when the system administrator is absent.

At a minimum, all system or application changes made by the programmer should be logged and reviewed. Presently, the system logs when anyone signs on or off the system, but makes no record of what that person does while on the system. That log is not reviewed unless a problem is identified or improprieties are suspected.

In order to ensure all changes made by the programmer are appropriate, all changes made by him should be logged, and reviewed and approved by TRD management.

Recommendation #1
We recommend the division:

A. Remove programmer access to production programs and data, or

B. Log and review all changes made by the programmer.

Access to Critical System Files and Programs Should be Controlled

For individual files and programs, different levels of access (read, write, execute, and delete) may be allowed within four different categories (system, owner, group, or world). The "system" category allows access through highly-privileged system accounts, usually available to the system administrator and security officer. "Owner" allows access to the user that originated the file. "Group" allows access by anyone associated with the specified group, and "world" refers to all users with access to the system.

During our review, we found read, write, execute and delete access is granted to system users through "Group" and "World" accounts,

which in effect, gives all users unlimited access to these files. The files include production data files, batch execution files, and programming source code. Improper changes or deletion of these files could cause major disruptions to the daily operations of TRD. Division personnel agreed the access allowed through "world" and "group" may be inappropriate. Write and delete access by "world" should be eliminated for critical files. The need for access by "group" and "owner" should be reviewed, and write and delete access deleted if not needed in the performance of their jobs.

Recommendation #2

We recommend the division review access to critical system files and programs, and remove write and delete authority from all users not needing it to perform their jobs.

Disaster Recovery Plan Should be Documented

The division has not completed a formal disaster recovery plan to return the application to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a timely manner, and minimize losses due to computer down-time.

Industry standards suggest management develop formal procedures to efficiently recover computer processing activities to normal operations following a disaster. The Montana Operations Manual (MOM) section 1-0240.00, outlines agency responsibilities regarding disaster recovery. These responsibilities include assigning recovery team member responsibilities, assessing information and resource requirements necessary to maintain applications, and determining alternate procedures which may be necessary if recovery is not timely.

As outlined in MOM section 1-0240.00, a disaster recovery plan may include but is not limited to:

- An inventory of current applications, operating system programs, telecommunications programs or networks, and hardware.

- An analysis to determine application significance and impact of loss, to define mission-critical applications which must be recovered.
- An analysis to determine application recovery priority.
- Selecting a disaster recovery method based on how long the organization can operate without processing, management's backup procedures, and cost.
- Identification, involvement, and commitment of employees responsible for operating applications.
- Definition of application requirements including personnel, hardware, system support programs, communications, data, special forms, etc.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a complete disaster recovery plan which defines division responsibilities and requirements, the division may be unable to recover its applications in a timely manner. The division has a document which contains a "problem reporting" phone number, hardware serial number, and software version numbers. However, other specifics, as outlined above, are not included in the document.

Recommendation #3

We recommend the division document and test formal disaster recovery procedures for the computerized application.

Documentation

Documentation provides a means for ensuring continuity of operations, and facilitates staff training. All parts of the system should be documented, from the system design and implementation, to the daily tasks performed by division staff. Documentation provides a level of support and reference to existing staff, and a starting point for training new or replacement staff in the event of employee turnover.

We found areas in the TRS operations where documentation could be improved. Things such as disaster recovery, systems enhancements and application changes, detailed system security guidelines, and individual employee workflow were not completely and clearly documented.

Division personnel indicated the documentation was not done primarily due to lack of resources and low priority. In addition, the contract programmers did not provide program or system operations documentation, as required in the contract, and will no longer provide support for the system after December 1999.

Recommendation #4

We recommend TRD review present policies and procedures, and ensure critical processes are thoroughly documented, to ensure continuity of operations.

Chapter III - Application Controls

Introduction

Application controls are related to the specific tasks performed by TRS's computer-based system. The major functional areas of the system can be broken down into the following three categories: 1) Contributions; 2) Maintenance of Member Accounts; and 3) Disbursements. Significant and material dollar amounts are processed by TRS. During FY97, distributions exceeded $92 million and contributions exceeded $81 million.

Application controls consist of a combination of manual and automated procedures. Input controls ensure data input is authorized, all authorized data is input, and all data input is included in processing. These procedures, along with proper assignment and control of access privileges to the system, help ensure the overall integrity of data input, processed, and maintained on the system.

We determined that application controls generally provide for controlled processing of TRD's computerized application. However, we found one area relating to access where controls could be improved.

Access Controls Over Application Functions

As part of internal controls over the various functions in TRD, the division has segregated certain tasks so that critical input and processing functions require the review and input of more than one person. This reduces the risk of inaccurate information being input onto the system, and also prevents any one person from having the ability to input fictitious or inaccurate information onto the system. For instance, one person inputs contribution totals from the school districts, and another person inputs the detail of the contributions. If the totals calculated electronically from the detail do not agree with the totals input manually, the system will not allow posting of the contributions until the difference is resolved.

Although the functions are segregated organizationally, the division has not implemented controls to ensure these conflicting duties are electronically segregated. Using the above example, the same person has the access to input both the totals and the detail, bypassing the internal control. The computer-based application gives the division the ability to separate those functions electronically, so each

individual has access to perform only one of the two tasks, and is locked out of the other. Division personnel indicated they did not feel electronic restrictions are necessary, because the individuals doing those jobs are aware of which tasks they are and are not authorized to perform. The division should implement the available electronic controls in coordination with their established organizational controls.

Recommendation #5

We recommend the division implement electronic controls to ensure no one person has the ability to perform incompatible and/or conflicting duties.

Agency Response

TEACHERS' RETIREMENT SYSTEM

1500 E. SIXTH AVENUE
PO BOX 200139
HELENA, MONTANA 59620-0139
(406) 444-3134
MARC RACICOT, GOVERNOR
STATE OF MONTANA

March 12, 1998

Scott A Seacat
Legislative Audit Division
P O Box 201705
Helena MT 59620-1705

Dear Mr. Seacat:

Attached is the Teachers' Retirement System response to the audit report on the Teachers' Retirement System computer based application. Generally, we have concurred with the substance of the audit recommendations, ie, restricting access to critical files or programs, documenting a disaster recovery plan and documenting application controls.

Thank you for the opportunity to respond to the audit report.

Sincerely,

David L. Senn
Executive Director

DLS/poc

"AN EQUAL OPPORTUNITY EMPLOYER"

Response to Audit Recommendations

Introduction:

The TRS converted to the current computer-based application in Sept of 1993. The system is nearly 5 years into production. During this time, the TRS has experienced personnel turnover in nearly 50% of the office positions. Our control and security model is based on several factors, not limited to electronic controls, but also including direct public interaction, actuary valuations inter-office practices and self-audits. Throughout the last 4.5 years we mailed out over 80,000 member statements of account, 35,000 1099R's, and 16,000 letters of correspondence all detailing individual account balances account activities, account status, and payment disbursements. TRS has been through four legislative audits, two actuary valuations and one federal compliance audit. Not once has our system been comprised or provided altered or false data. This is not accidental it is a direct result of an adequate security model. By today's industry standard, the life expectancy of an application is around 5 years.

The TRS is a closed system (not publicly accessible) and only supports one tightly integrated application for 12 Helena based users. The very nature of the application integration helps identify problems and errors because each program of the application depends heavily upon other programs and electronic controls to operate correctly.

Recommendation #1.

We recommend the division:

A. Remove programmer access to production programs and data, or
B. Log and review all changes made by the programmer.

TRS does not concur with the recommendation.

No significant risk is involved with the contract system programmer having access to the TRS data and production database since other compensating controls would prevent or discover any unauthorized changes. Although the programmer has technical knowledge of the system, he has no physical access to the office and no knowledge of our operational procedures. Since all disbursements from the TRS are based on data which is reported to and stored in the office, this is a physically control which prevents and or discovers any direct data alteration. The programmer can absolutely make no changes in status or payment for any retiree or beneficiary and go unnoticed because of the internal controls and manual verification with outside reports and/or employer supplied documents.

Currently, TRS logs and tracks the entry and exit times of the contract programmer. This log is available for review and can be used in conjunction with other system tools to diagnose problems or track errors back to the contracted programmer if needed. In addition, all

changes to individual accounts made through the application are logged by the system.

The TRS relationship with the contract programmer is the same relationship that has existed with previous programmers for TRS, which worked for the application support bureau of the state ISD. These programmers also had complete access to raw data, test programs and production programs. This relationship still exists today among many state supported systems and indicates a defacto computer standard; hence, an industry standard.

Recommendation #2.

We recommend the division review access to critical system files and programs, and remove write and delete authority from all users not needing it to perform their jobs.

TRS partially concurs with the recommendation.

Neither the world nor group have any access to any critical system files (operating system files.)

TRS agrees with this recommendation in reference to program files and has modified all critical executable programs to the security of read and execute.

Because of the tight integration of the single TRS application and the software used (Powerhouse) any corruption or deletion of executable files is immediately noticeable and would not cause any major discrepancy as stated in the report. TRS would simply restore the file completely from our nightly backup and make incremental updates from our transaction journals and logs, which monitor and log all file updates.

Recommendation #3.

We recommend the division document and test formal disaster recovery procedures for the computerized application.

TRS partially concurs with this recommendation.

The disaster recovery procedure identified in the audit report includes inventories, loss analysis, recovery priority and methodology, employee involvement and identification and definition of application requirements.

TRS has in place a system management document, a security manual and an inventory document which together outline the system support/recovery contacts, critical phone numbers, software versions, support agreement access codes and hardware serial numbers.

We separately store all software version licenses. Our current support agreements guarantee the on-site response to system problems or failure within 8 hours. TRS verifies and tests our system backup and restore procedures every 3 months.

We are confused by the recommendation since our multiple documents and single application design (which is either operational or not) covers all aspects of the MOM requirements, just not in one document. If the recommendation is to document the current procedure in one manual, we concur. Consequently, TRS will review the MOM section 1-0240.00 and incorporate into the system management manual all pertinent recovery information or procedures.

Recommendation #4.

We recommend TRD review present policies and procedures, and ensure critical processes are thoroughly documented, to ensure continuity of operations.

TRS does not concur with this recommendation.

State on page S-4 of the audit report, the areas of documentation which could be improved include disaster recovery, systems enhancements and application changes, detailed security guidelines, and individual employee workflow.

Disaster Recovery: See response to recommendation #3.

Systems Enhancements and Application Changes: All enhancements made to the application are documented and logged inside the program. All changes made by the contracted programmer are also documented through an enhancement request form and documented through a verification fax when work is completed by the contracted programmer. TRS feels this is adequate.

Detailed Security Guidelines: TRS maintains a security document which supplements the Department of Administration security guidelines MOM section 1-0250.00 and the Administration memo dated 10/17/96. TRS feels this is adequate.

Individual Employee Workflow: TRS has a complete data flow diagram of the existing system, a database design schema and updated position descriptions. TRS feel this is in conjunction with on-line help screens is adequate.

The current system is adequately documented. System documentation is available both on-line and in manuals. TRS has experienced significant turnover in operational positions over the last four years and the documentation has proven to be adequate for position training, cross training of positions and in-house development of system programs.

Documentation of systems is a very subjective view and can always be changed or improved depending on who is looking at it. TRS has been in a series of negotiations with the contractor to provide a more enterprising set of documentation. It was not until October of 1997 that the vendor decided not to provide the documentation ...consequently TRS withheld

$15,000 from the final payment of system documentation. As new modules are developed or as enhancements occur, TRS will review the documentation and update as necessary.

Recommendation #5.

We recommend the division implement electronic controls to ensure no one person has the ability to perform incompatible and/or conflicting duties.

TRS does not concur with this recommendation.

The TRS control and security model is based on several factors, including but not limited to electronic controls. TRS has electronic controls in place in conjunction with physical and operational controls. We utilize application security, module security and screen security to provide an adequate amount of electronic control. The TRS is a small organization and many of our jobs and operations overlap. This overlap creates an extremely effective and efficient work environment. To tighten down controls needlessly would be detrimental and inefficient.

TRS believes the current system has the electronic controls as required by industry standards and there are compensating physical and/or operational controls to protect all data and cash flow integrity. The TRS system internally logs all changes to individual accounts and records the pertinent data to identify whom performed the update, this log is not viewable or changeable by any TRS employee. Despite the recommendation claim, no employee physically involved with a money transaction has the ability to input both the detail and totals for any report procedure. All TRS money transactions are approved or verified by a removed TRS employee. In the event that an employee fills in for the absence of a co-worker who handles money, his/her electronic access security is modified to prevent dual access. This internal control was tested and verified by the auditor Alan Lloyd when the accounting clerk was out and the refund clerk filled in for her.